Hard_EnglishPassage_3018
Cybersecurity and the Digital Data Protection

Words: 463, Characters: 3426 **LEVEL: HARD**

The rapid penetration of high-speed internet networks and the exponential growth of 83
the digital economy have fundamentally revolutionized the way modern societies 162
communicate, conduct financial transactions, and manage administrative operations. 245
As government services, banking institutions, and private enterprises migrate their 329
critical infrastructure to cloud-based servers, the overall efficiency and accessibility of 421
services have improved dramatically. However, this massive digital transformation 503
has also exposed the global economy to unprecedented vulnerabilities in the form of 587
sophisticated cyber threats. Today, data is universally recognized as the most valuable 675
commodity in the world, often referred to as the new oil. Consequently, organized 757
cybercriminal syndicates and state-sponsored hackers are continuously developing 838
highly complex malware, ransomware, and phishing techniques to steal sensitive 917
personal and financial information. A ransomware attack, for instance, maliciously 1000
encrypts a victim's database, and the hackers demand a massive ransom payment, 1079
usually in untraceable cryptocurrencies like Bitcoin, in exchange for the decryption 1164
key. Such severe cyber-attacks can paralyze the operational capacity of crucial 1244
national assets, including power grids, healthcare systems, and aviation networks, 1327
thereby posing a direct threat to national security. To effectively counter these digital 1417
threats, the government established the Indian Computer Emergency Response Team 1497
(CERT-In), which acts as the national nodal agency for responding to computer 1575
security incidents as and when they occur. While technological defense mechanisms 1657
like firewalls and multi-factor authentication (MFA) are essential, the legal framework 1745
governing cyberspace must also continuously evolve to keep pace with rapid 1820
technological advancements. The Information Technology Act, originally enacted in 1902
the year 2000, was the first major legislative attempt to provide legal recognition for 1990
electronic commerce and define cybercrimes. However, as the digital landscape 2068
became more complex with the rise of social media platforms and artificial 2143
intelligence, the need for a comprehensive privacy law became absolutely critical. 2226
Following years of intense public debate and expert consultations, the parliament 2308
successfully passed the Digital Personal Data Protection Act in August 2023. This 2390
landmark legislation fundamentally shifts the balance of power back to the individual 2476
citizens, legally defined as "Data Principals," by giving them greater control over how 2564
their personal information is collected, processed, and stored by large multinational 2650
technology corporations. The act explicitly mandates that companies can only collect 2735
data after obtaining clear, affirmative consent from the user, and they must 2812

implement robust security safeguards to prevent any accidental data breaches. **2890**
Non-compliance with these strict privacy guidelines can result in massive financial **2974**
penalties running into hundreds of crores. As we navigate the complex uncertainties **3058**
of the digital age, it is absolutely essential to cultivate a strong culture of cyber **3144**
hygiene among ordinary citizens. Basic digital literacy, such as identifying suspicious **3232**
email links, using strong and unique passwords, and regularly updating software **3312**
applications, is the first and most effective line of defense against financial fraud and **3402**
digital identity theft. **3426**